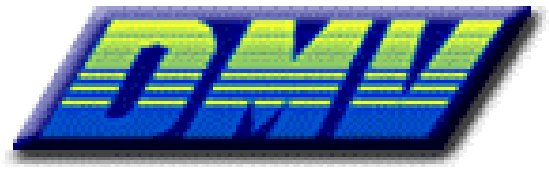
Created on 2/27/2002



VPN Service Offerings V2.7

Introduction

Customer-provided data is critical for DMV to effectively perform many of the functions delegated to it either through legislation or other requirement. This may include data relating to Parking Violations or Insurance Update information or any number of other data sources. DMV is committed to continue to support our customers with the information processing services they require to meet their goals. However, in order to remain competitive in providing our customers with the highest quality services available, it becomes necessary to phase out services that are no longer technically or fiscally feasible. DMV's support of Reel Tapes is one of the services that are becoming increasingly harder to support. Costs to maintain both hardware contracts and to purchase additional hardware are becoming prohibitive for DMV's continued use of this service. Additionally, service providers are no longer supporting Reel Tape Services. Therefore, DMV will be phasing out Reel Tape services by providing VPN Network Services. These VPN Network Services, besides allowing us to phase out Reel Tapes, will provide additional benefits such as allowing other DMV processes to be converted to VPN in the future.

The VPN Services that will be offered to DMV customers will provide a secure line of communications to an FTP Server. Customers will then securely transmit data that otherwise would have been sent to DMV via Reel or Cartridge Tape. While this initial phase is deliberately intended to phase out Reel Tape Services at DMV, it is our intention to provide in the future, other DMV services via VPN Network connections. We are excited about the new service offerings we are preparing for our customer base and look forward to providing new and better services to you, our valued customer.

Intended Audience

This document is intended for Managers, Professionals, business decision-makers, and organizational change-agents. Our goal is to provide an overview of the VPN technology, its implementation, its security, its reliability, and DMV's utilization schema for this technology. In-depth technical specifications and analysis will be handled by a separate document directed toward technical personnel.

The purpose of this document is to present DMV customers with an accurate information source that outlines the availability of VPN Services through DMV Systems. For the purposes of this document, Services refer to *both* Networking and Processing; services such as internetwork communications and those that are typically associated with DMV applications such as DL Inquiry or Court Abstracts. This document will present Networking services available to our customers for interaction with DMV systems and present the necessary requirements for accomplishing such services. We also include the necessary forms for adding any of the services presented herein into your portfolio, and provide contact information for any questions that you may have regarding the services presented in this brochure.

We are striving to better meet the needs of our customers through innovative programs and request that you take a moment and fill out the Customer Questionnaire located on page 17 of this brochure and return via fax or mail to the department. Thank you for your input on how we can improve our services.

VPN Technology

The technology that has enabled today's VPN product base has been available for a number of years in the form of Permanent Virtual Circuits (PVC's) in the circuit switched and frame-relay networks. The ability to apply the theories associated with PVC tunnels on these networks yields the VPN solution. The addition of strong security (which we will define as the ability to transmit data from one verified host to another verified host in a manner that keeps the data unreadable to eavesdropping and invulnerable to spoofing) provides us with the possibility of securely transmitting sensitive data over the Internet in an apparent virtual Tunnel or a VPN.

While this technology is more security and management intensive than the implementation of say, a leased-line, when you consider the full spectrum of benefits associated with the technology, VPN is a cost-effective solution for both the implementer and the benefactor of that implementation (the RA or EPA Client) as in the case of Extranet and Remote Access configurations. We hope that you will agree with us and look forward to your utilization of this service.

Implementation

Virtual Private Networks have the ability to be implemented in a semi-transparent manner depending upon network infrastructure and architecture. For instance, there is no need to procure dedicated data services (circuits as with leased-lines), no need to reassign bandwidth from existing services (as adding voice channels to your existing T1 Circuit), and no need to purchase new hardware or software (depending on the solution chosen).

At DMV, we have made implementation as simple as loading a software client onto a PC that you already own and making simple adjustments to allow proper connectivity. This PC will utilize your existing Internet connectivity to establish a Secure Tunnel (IPSec Tunnel) to DMV's VPN Concentrator and allow for data transmittal. There are no charges associated with the use of the Client Software and we manage security implementation on our end of the connection through Policy pushed to the Client PC. Your personnel will simply have to know how to use the PC and have the ability to extrapolate the data that they intend to share with DMV.

Additionally, we've set-up Pre-Installation Technical Supportto handle your questions or concerns that you may have both prior to implementation and at technical analyst that will be assigned to you for the VPN installation process and implementation of application programs. We'll be there to support our solution to you.

Security

Security of the VPN Tunnel is a 3-fold system to ensure client integrity, user integrity and data integrity. Each of these aspects will be explained in the paragraphs that follow.

The first security consideration deals with client integrity. With this comes the concept of non-repudiation; the ability to positively identify the (Computer) sender of specific data so that it does not come into question whether a (Computer) sender is the true sender

of data. This is necessary to keep your network invulnerable to client spoofing or in more accurate terms, client identity theft. This is accomplished through the utilization of 2 authentication algorithms that are installed within the VPN Concentrator and a predefined IPSec Security Association. In essence, this provides for both the client and the VPN Concentrator to have the ability to positively identify the other via cryptographic mathematical calculations performed on data received from the other end of the communication channel. These calculations must arrive at the same conclusion based on the secret knowledge that each knows in order to confirm the others' identity. This is done each time the IPSec Security Association is established.

The second security consideration is user integrity. This is accomplished both through application security measures (i.e. RACF user accounts) and through the use of a RADIUS authentication server on the concentrator end of the VPN tunnel. This provides that even if a Client machine were compromised (either through cracking or man-in-the-middle attack) that the user would need to know at LEAST 2 separate and distinct usernames and passwords that WILL change frequently and have no direct correlation to the end-user (i.e. MSMITH will NOT be a username for Mary Smith). This will further ensure that the data between sources remain secure.

Finally, the concept of data integrity is handled at both the software and hardware level in the current configuration of the DMV VPN solution. We use 168-bit Data Encryption Standard (3DES) and vary the implementation (i.e. EEE3, EDE3, etc.) of this schema at different times to further decrease the likelihood of encryption compromise. This is done at the software level on the client end of the connection (in a RA configuration) and done at the hardware level on the VPN Concentrator side of the connection (or at both ends of an EPA configuration). The implementation of these standards and our willingness to continually update and vary their implementation produces a strong encryption and authentication schema that provides us with the strongest level of data security available. We are certain that your technical staff will agree and we look forward to further in-depth consideration of such issues with your organization.

Reliability

The reliability of the VPN solution is based on several factors. Some will be under our control, others will be the responsibility of the customer; all will have impact on the VPN Solution.

The factors under our direct control are the hardware and the software associated with the VPN solution at DMV's end and the customer end of the connection. DMV will maintain all software at the customer end. This will include updates to the software as they become available. DMV will actively monitor the VPN Concentrator and its connections for service quality and we'll expedite quality of service of VPN Traffic on our internal Network. DMV will actively and passively monitor the security of the VPN solution 24-hours a day through both our internal systems and through Service Level Agreements with our service providers. Essentially, DMV will act responsibly to our customers to be able to provide a reliable service that will be available when our customers expect service availability. We will, of course, maintain our VPN Concentrator and associated equipment at appropriate times and within established

maintenance windows. DMV will have maintenance windows on the VPN Solution and these will be communicated in ample time to the affected customers as we establish appropriate times for maintenance to occur based on end-user usage patterns (usage patterns will have to be established before we determine windows).

The Internet itself, although out of our control, provides us with a reliable transport medium for our VPN Solution. The Internet is one large network in a meshed topology. This mesh topology provides us with a network with built-in redundancy with several thousand possible routes to a single host on the Internet. This redundancy was one of the factors that encouraged governmental interest in the Internet in the late 1960's and early 1970's. Today, it is the main reason the Internet has such resilience. Since we utilize this as our primary transport medium for our VPN Solution, we're fully taking advantage of the Internet's resilience and redundancy.

Unfortunately, because of the distributed nature of the Internet, we cannot maintain Quality of Service or Internet connectivity from end-to-end on the VPN Solution. We can only ask that customers have ample Service Level Agreements with their Internet Service Provider (ISP) to ensure service availability when the customer demands such services. This however is mitigated by redundancy detailed in the previous paragraph. We don't anticipate any extended problems in our ability to utilize the Internet as our primary medium for passing IPSec traffic on our VPN Solution.

DMV's Services

This section will provide you with detailed information regarding the Networking and Application Services available to our customers, as those services relate to VPN Internetworking. The customer requirements for each of the solutions presented are different and should be considered carefully. Technical contacts will be required for any solution selected and an in-depth analysis performed prior to commitment to implementation.

Networking

This section details the VPN Networking options currently available to DMV customers. The table below will help you quickly determine which option is best suited to your needs. VPN Client Access is a single-PC solution best suited to small network and Extranet Partner Access is a router-to-router solution best suited to larger network environments. Please refer to the appropriate section of this document for full details on each of the VPN Networking options contained in this table.

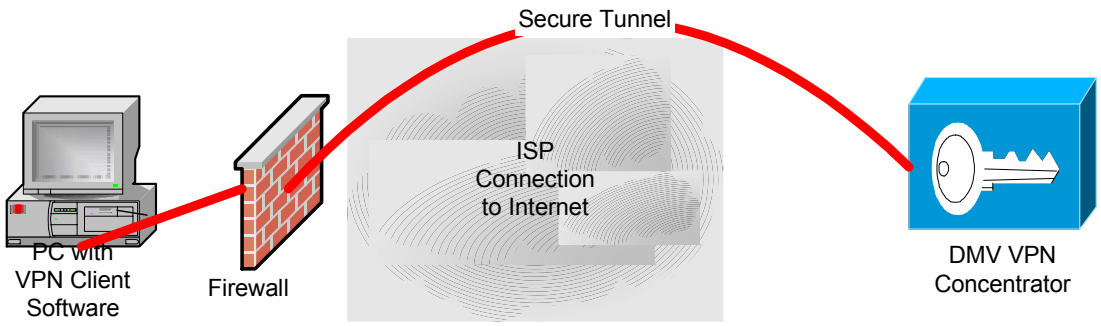
Table 1

	VPN Client Access	Extranet Partner Access
Easy to Implement/Use	Yes	No
Additional Customer Provided Equipment Required	No[1]	Yes[2]
Multiple PC's Supported	No	Yes
Security Standards	3DES, HMAC/SHA-1	3DES, HMAC/SHA-1
Availability	Yes	Yes
Batch Processing Supported	Yes	Yes
Online Processing Supported	No	No

[1] Provided Customer equipment meets Minimum Standards.
[2] Routers and IOS Software must be VPN compatible.

Remote VPN Access (VPN Client Access)

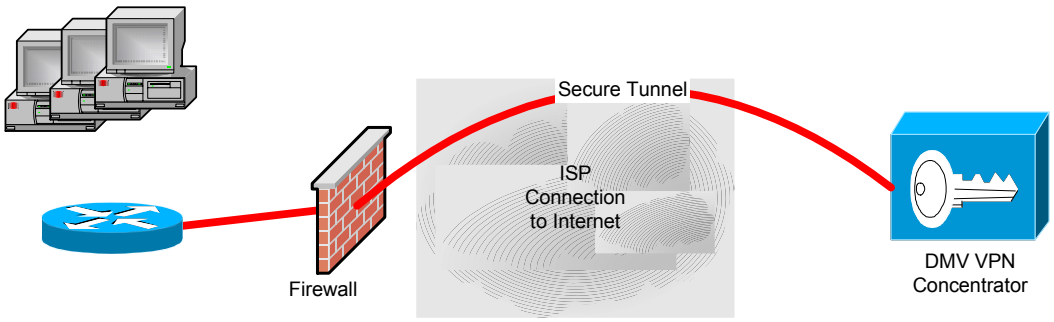
The Remote VPN Access solution provides secure communications for DMV customers via the customers own IS connection to the Internet. Remote VPN access is accomplished through the use of a VPN Client (Client) that runs as a software program on customer owned personal computer (PC) equipment. The Client creates a secure connection between the PC and the DMV's VPN Access Point using an encrypted tunnel. The illustration below depicts the VPN Remote Access scenario.



This solution is ideal for customers, who have small volumes of data, transmit infrequently, or who only have a limited amount of bandwidth or network infrastructure. This solution will allow customers to retire their magnetic tape equipment without incurring any new costs. Because of the ease of use and ease of implementation of this solution, this will be the most popular solution for our smaller customers. This would also provide a viable solution for larger customers who transmit larger amounts of data on an infrequent basis. Please consult the DMV for Pre-Installation consultation on the best solution for your organization.

Extranet Partner Access (EPA)

VPN Extranet Partner Access (EPA) or router-to-router access also provides secure connectivity to DMV customers via the customers own ISP connection to the Internet. However, because the EPA solution is a Hardware-based to Hardware-based VPN solution, it requires specific hardware and software to be maintained on the customer end at the customer expense. The EPA solution creates its secure connection between the customers Border Router and DMV's VPN Concentrator, again using an encrypted tunnel. The illustration below depicts the EPA Access scenario. A benefit of this solution is the ability of the concentrator to create multiple tunnels to multiple end-users.



The benefit of this solution is evident to our larger customers who have an installed network infrastructure. It provides access to the DMV VPN Concentrator via a single IPSec Tunnel configured from the customer router to the DMV VPN Concentrator. This solution allows for any number of hosts (PC, Midrange, Mainframe or other system) to connect to DMV's FTP servers via a single tunnel. This consolidates management to a single device and provides access to any number of systems at the customer site. This scenario requires specific hardware and software at the customer site, purchased and maintained by the customer. DMV will still subject the IPSec tunnel to DMV's Policy-based Management System. Technical staff will be required to implement this solution with DMV acting as a resource.

Applications

This section lists the Application Programs (AP) available to our customers via VPN Networking Services. Note that some services are available and others are in conversion. The current focus of AP is the reduction in magnetic tape usage. Table 2 below outlines the Application Programs available to DMV customers.

Table 2

Application Program	Code	Type	Availability	Type of Service
Daily Inquiry	RR8096	VR	YES	Batch
Daily Inquiry	RR9096	VR	YES	Batch
Daily Inquiry	DR2017	DL	YES	Batch
Daily Parking	RC7016	VR	YES	Batch
Monthly Parking	RC7837	VR	YES	Batch
Daily Court	DC0716	DL	YES	Batch
Company Records	RC2026	VR	YES	Batch
Company Records	RC2926	VR	YES	Batch
Daily Insurance	DM0816	DL	YES	Batch
Semi-Annual Jury Selection	DM2556	DL	YES	Batch
Monthly PFR	RP0236	VR	In-Conversion	Batch
Monthly Vessel	BC3037	VR	YES	Batch
Monthly Tax Delinquent Vessels	BC1496	VR	YES	Batch
Employee Pull Notice Add/Delete	DR4196	DL	YES	Batch
Employee Pull Notice Print	DR2017	DL	YES	Batch
Permanent Fleet Registration	RP2496	VR	In-Conversion	Batch

Non Priority Listing Detail 1

Customer Requirements

General Requirements

Item	Description	Comments / Reference location
1	All data transferred to/from DMV MUST terminate behind an internal firewall AND the system MUST be protected AND on a trusted network. DMZ configurations do NOT meet this requirement.	VPN Service Offerings Manual, reference the Table of Contents (TOC).
2	VPN batch customers must change their Resource Access Control Facility (RACF) password at least every 35 days.	VPN Client Manual, reference the TOC.
3	Additional RACF password standards are: Passwords 1) must be at least 5 characters long. 3) can be any combination of alphabetic, numeric or special characters. 4) cannot be reused for 32 iterations. 5) will be locked out of the system after 5 erroneous password attempts. 6) can be changed any time.	
4	Review the minimum hardware/software requirements.	VPN Service Offerings Manual, reference the TOC
5	Security requirements require 3DES encryption for Router-to-Router customers.	VPN Service Offerings Manual, reference the TOC.
6	Firewall and network configuration changes may affect your VPN connections. Our technical staff will assist when possible.	This applies to both Router-to-Router and Client Software.
7	As technology improves/changes, additional security concerns and changes may be required. Those can include, but are not limited to: downloading new client software, changing RACF passwords, new security requirements, etc.	VPN Service Offerings Manual, reference TOC.
8	The courtesy e-mail notification has limitations. It is the user's responsibility to retrieve all data.	Due to network configurations, some customers may not be able to receive e-mail notifications.
9	All documents must be completed before starting the VPN technical implementation phase.	Contact the Information Services Branch (ISB) for further information.
10	Assess your requestor codes and processes with ISB before submitting your questionnaire.	Contact ISB for further information.
11	There are program limitations for the VR Non-Urgent Inquiry and VR Vessel Extract Programs, specifically variable vs. fixed blocked data. A program change is required to change the output from variable length to fixed length format.	Programming changes may delay the implementation of the VPN process. Contact ISB for copies of record layouts.
12	Output data set names are emptied and reallocated recurrently. Therefore, customers must retrieve their output files prior to sending their input files.	This applies to daily and weekly processes. Monthly output files are normally available for at least 2 weeks.
13	There is a maximum limit of 50,000 records that a customer can send for each process, per day. Anything larger must be coordinated in advance.	This limit helps our staff to schedule all jobs. Anything larger than 50,000 records, must be coordinated with the VPN technical support staff.
14	Input files are processed Monday through Friday, excluding DMV non-business days (holidays, weekends, etc.). The DMV holiday schedule is on the web site under DMV Locations and Hours – see http://www.dmv.ca.gov/about/holidays.htm	If you have an automated process, make sure your input files have been processed before sending newer files to avoid overwriting your own input data.
15	The daily production schedule begins at 4:30 p.m.. Input files sent by this time will be available the next business day, by 07:00 a.m.,.	All times referenced are Pacific Time.
16	There will be no record layout changes other than the exclusion of the header and the trailer labels that are characteristic of tape processing only.	Contact the VPN technical support staff for further information
17	**EPN Customers Only** – The date and a unique identifier of the individual reviewing the driving record must be placed on the electronic records received from DMV. The identifiers must be permanent and unalterable.	Contact ISB for further information

All VPN Connections

Pursuant to Government Code and DMV Policy, all VPN Connections must, at a minimum, meet the following requirements in order to protect the integrity and confidentiality of DMV data. These requirements apply to ALL VPN connections, including router-to-router, LAN-to-LAN, and client connections.

- At least one firewall system must be located between any server that hosts applications, provides access to or stores DMV information and each external network entry point.
- Firewalls must include, at a minimum, provisions for packet filtering, application gateway security mechanisms, and circuit-level gateways.
- If a server is accessed through the same Internet access point used to access the Internet from internal workstations, the firewall implementation must also include proxy services and/or address translation.
- When a server is used to store, transmit, or process DMV information, the firewall systems employed must be located so that all communications with the Internet must pass through two differently-authored firewall systems separated by an isolated network.

Single VPN Client

The Single VPN Client is again a software solution that operates on a PC at the customer site. The customer owns this PC however; this PC must meet the Minimum HW/SW Requirements outlined below. While this is customer equipment, the DMV reserves the right to enforce security standards on the Client via policy enforced by the VPN Concentrator. This is necessary to ensure both customer data integrity and DMV systems security.

Minimum HW/SW Requirements

Pentium Class Microprocessor – or better

Microsoft Windows95 OSR2 (w/MS DUN 1.3)	16 MB RAM
Microsoft Windows98	16 MB RAM
Microsoft Windows 98 SE	16 MB RAM
Microsoft Windows ME	32 MB RAM
Microsoft Windows NT 4.0 SP3	32 MB RAM
Microsoft Windows 2000	64 MB RAM
Microsoft Windows XP	128 MB RAM

Direct Network Connection – DSL/Cable/Modem or interface card configured to access the Internet via either a network connection or through a dial-up connection to your Internet Service Provider.

Batch Type Services

All batch processes currently available will utilize the File Transfer Protocol (FTP) installed as a service with TCP/IP on the customer PC. There are currently no caveats to utilizing this protocol over VPN. If you require assistance prior to full implementation at your site, please contact the Pre-Installation Contact contained within the DMV Contact Information section of this document. After implementation you may contact Post Installation Support also contained in the DMV Contact Information section of this document.

Multiple VPN Clients

Multiple VPN Clients is again a software solution that operates on PC's located at the customer site. The customer owns this PC equipment; however, the Minimum HW/SW Requirements outlined in the Single VPN Client Section continue to apply for each PC to be utilized. While this is customer equipment, the DMV reserves the right to enforce security standards on the Client via policy enforced by the VPN Concentrator. This is necessary to ensure both customer data integrity and DMV systems security.

Single Router-to-LAN Connection

The Single Router-to-LAN Connection is a hardware/software solution that operates on a router located at the customer site. The customer owns and maintains this router; however, it must meet the specifications outlined below. While this is customer equipment, the DMV reserves the right to enforce security standards on the router via policy enforced by the VPN Concentrator. This is necessary to ensure both customer data integrity and DMV systems security.

Minimum Router HW/SW Requirements

Cisco VPN Capable Router*

Appropriate Revision of Cisco IOS Software on VPN Capable Router*

Direct Network Connection – Ethernet or WAN connection to the Internet via ports on the router. The interface may at the customers' discretion pass through a firewall. DMV will develop the configuration needs associated with this solution after careful consideration of the customer network infrastructure and configuration.

* Specific Router and IOS information will be reviewed at time of request.

Batch Type Services

All batch processes currently available will utilize the File Transfer Protocol (FTP) installed as a service with TCP/IP on any customer equipment. There are currently no caveats to utilizing this protocol over VPN. If you require assistance prior to full implementation at your site, please contact the Pre-Installation Technical Support contained within the DMV Contact Information section of this document. After implementation, all service calls should go directly to the Post Installation Support also contained in the DMV Contact Information section of this document.

Service Request Forms

Forms for requesting DMV's VPN Service will be provided by DMV's Information Services Branch (ISB). All forms should be filled out entirely and returned to the appropriate address denoted on the forms provided by ISB. If you need to contact DMV for the forms, please contact the VPN Business Coordinator at (916) 657-5582.

DMV Contact Information

Pre-Installation

For Pre-Installation Technical Support or for general questions prior to implementation, please contact the following number.

Pre-Installation Technical Support	(916) 657-8861

Post-Installation Support

You will be assigned a technical analyst for the VPN installation process and implementation of Application Programs that you have specifically requested through our business office. **Any questions or trouble calls can be directed to the technical analyst.** If you need a password reset refer to the number below.

Password Reset Only	(916) 657-7915

Customer Questionnaire

We appreciate your taking the time to communicate with DMV. DMV looks forward to continued service with you, our valued customer.

Please circle a number after each question using the scale below.

	Fully Agree		N/A		Fully Disagree
This brochure answered my questions.	1	2	3	4	5
I intend to utilize the services outlined in this brochure.	1	2	3	4	5
I found the information I needed in this brochure.	1	2	3	4	5
This brochure is accurate and free of errors.	1	2	3	4	5
This brochure is written at a correct level of complexity.	1	2	3	4	5
I am satisfied with this brochure.	1	2	3	4	5

Additional Comments

_____

_____

_____

We thank you for taking the time to communicate with us, you can either fax or email this survey to us at one of the addresses below.

Please fax to: DMV – ISD
Attn: VPN Coordinator
Fax: 916-657-6581

Or email to: psgmail@dmv.ca.gov

Customer Name					
Company Name					
Mailing Address					
City		State		Zip	
Telephone Number	( )	Email			

Glossary

This glossary contains terms as they are utilized in this document. Please note that this may not be the only application of any such terms.

3DES Triple Data Encryption Standard. A mathematical algorithm applied to data in order to encrypt the data. The application of the 56-bit Data Encryption Standard applied to any given amount of data. This standard produces a 168-bit strong encryption schema that can be varied according to the way in which the 3DES standard is applied.

AP Application Program. Any program currently offered through DMV to our customers over any currently supported medium.

Batch Batch is an off-line processing environment, usually running at night or the weekend, where long-running and resource-intensive jobs are run. DMV's batch environment is run on an OS/390 mainframe processor at Teale Data Center.

Circuit Switched The public switched telephone network in which circuits are dedicated to a single conversation. In the case of leased-lines, the circuit is dedicated from end-to-end, creating a permanent virtual circuit through the public switched telephone network.

Client The VPN Software that will be loaded onto a Personal Computer in order to access DMV's Virtual Private Network. Also, refers to a router or other VPN capable device located on the customer premise and owned by the customer.

Client Integrity The application of certain protocols and policies to ensure that the client communicating with DMV's Virtual Private Network is the trusted client that is expected. This is accomplished through the application of public/private keys and Security Associations.

Concentrator See VPN Concentrator.

Data Integrity The application of mathematical cryptographic algorithms to raw data in order to encrypt the data for transport across the un-trusted Internet in a manner that keeps the data secure from interception, eavesdropping, and other forms of data manipulation.

Dedicated Data Services Any of the dedicated data services typically associated with Wide Area Networking (WAN) Connectivity. Services might include 56k leased-lines, Frame-relay T1's, OC3 and other digital type services.

EPA Extranet Partner Access. Allowing business partners with a valid business reason limited access to parts of an internal network. This might be a 56k leased-line connection operating an RJE connection between business partners or as in the case of VPN, an FTP connection via IPSec Tunnel through the Internet.

Firewall Any combination of hardware and software, in combination with rules or policies that provide for segmentation of a network via different interfaces (one public, one private) in order to limit traffic on the protected network segment.

Frame-Relay A packet switching technique that allows for high speed data transmission between peers on the frame-relay network.

FTP File Transfer Protocol. A light TCP/IP protocol that allows the transfer of files over any medium (analog circuits to fiber optic cable). It is defined by the specific TCP/IP implementation and usually conforms to FTP specification as they have developed.

Internet The global internetwork of interconnected nodes that allows for speedy transport of information via packet and circuit switched services. The transport that will provide the connectivity for the VPN between DMV and Clients.

IPSec Internet Protocol Security. The Internet security protocol that specifies a network layer model of encryption and authentication of IP data packets. The standard includes the Authentication Header (AH) and the Encapsulated Security Payload (ESP) for authentication and confidentiality of TCP/IP packets.

ISB Information Services Branch. ISB has the responsibility of developing and maintaining policies, regulations and automation needs relating to the release of department record information.

ISP Internet Service Provider. Any commercial or non-commercial entity providing access to the Internet through any available access method. The ISP and agreements governing the ISP connection are the responsibility of the customer as it relates to this document.

Leased-line Any of the Dedicated Data Services that typically create an end-to-end connection via dedicated service circuits and dedicated equipment. This includes 56k leased-lines, T1, T3, and other such services. Typically these services are utilized in WAN services in a single corporation.

Nonrepudiation The process through which senders of data are positively identified via a complex cryptographic algorithm.

Online Online refers to an interactive session with a computer system via a terminal or other virtual access method. Online applications typically include applications such as TSO, an interactive session on a Unix Server or, other real-time applications that affect data instantly.

Policy The implementation of specific rules that will be enforced on any device connected to the VPN network. These policies are enforced by the VPN Concentrator and pushed out to each Client on the VPN network. DMV maintains these policies to protect both DMV systems as well as customer premise equipment from any malicious intent.

PSTN Public Switched Telephone Network. The circuit switched network that carries the vast majority of both voice and data in today's communications.

PVC Permanent Virtual Circuit. The creation of an end-to-end connection via a dedicated data service over the PSTN.

RA Remote Access. The process of allowing authenticated clients access to specific network resources via a remote access solution (i.e. dial-in or VPN).

RACF Resource Access Control Facility. IBM Mainframe security mechanism designed to secure the resources for which it is responsible.

RADIUS Remote Authentication Dial In User Service. Servers that are used for user authentication, authorization and accounting and for terminals that speak the RADIUS protocol.

RJE Remote Job-Entry. To submit a series of commands through a terminal or processor that has access to a computer through a data link.

Router A device that routes IP packets over an internetwork. The device uses routing algorithms to determine the best path for packets to reach their destination.

Security Association A unique communication setting used in IPSec that two end points use to define what parameters they are going to use, e.g., encryption protocols and authentication protocols.

Spoofing The process through which a person with malicious intent (cracker) makes it appear to affected systems that data is originating from a valid system. Also called Address Spoofing, the cracker effectively performs Internet address identity theft to appear to be a valid system to the cracked system.

Technical Analyst. DMV ISD's implementation of a helpdesk organization in support of the VPN solution being offered to our customers. All helpdesk calls will be routed through the technical analyst to determine the correct course of action to take on each call to ensure it is handled correctly and in a reasonable time frame.

Strong Security The ability to transmit data from one verified host to another verified host in a manner that keeps the data unreadable to eavesdropping and invulnerable to spoofing. Implementing several layers of security to protect data from interception, manipulation, and replacement in transit.

T1 Circuit A dedicated data service circuit providing 1.544 Megabits per second throughput over a standard copper medium on the PSTN.

TCP/IP Transmission Control Protocol/Internet Protocol. A suite of internetnetworking protocols based loosely on the International Standards Organization Open Systems Interconnect 7-layer reference model. It has been the standard for Internet traffic since the mid-1970's and continues to grow to accommodate new uses.

Teale Data Center The Teale Data Center is a state department within the Business, Transportation, and Housing Agency. Teale provides data, networking, and consulting services to state agencies.

Tunnel A logical connection between two hosts creating a virtual end-to-end connection between two hosts. The physical connection between the two hosts may be on a single network or traverse multiple networks or the Internet.

User Integrity The requirements imposed by DMV to require unique usernames and passwords and the requirements for customers to change said username and passwords as DMV requests. DMV will ensure that these usernames and passwords have no direct correlation to the end-user or their respective organization.

VAN Value Added Network. A private network provider or third party service provider that receives, stores, and transmits data, facilitates electronic data interchange (EDI) or provides other network services.

VPN Virtual Private Network. Any number of remote connectivity services that provide secure communications from end-to-end creating a tunnel.

VPN Concentrator Virtual Private Network Concentrator. The device that is installed at the DMV to enable VPN connections to multiple customer sites via the Internet. By its nature, a concentrator concentrates several similar connection types into a single network solution (i.e. one box vs. several VPN routers).